

# **PART 95—SECURITY FACILITY APPROVAL AND SAFEGUARDING OF NATIONAL SECURITY INFORMATION AND RESTRICTED DATA**

## GENERAL PROVISIONS

Sec.

- 95.1 Purpose.
- 95.3 Scope.
- 95.5 Definitions.
- 95.7 Interpretations.
- 95.8 Information collection requirements: OMB approval.
- 95.9 Communications.
- 95.11 Specific exemptions.
- 95.13 Maintenance of records.

## PHYSICAL SECURITY

- 95.15 Approval for processing licensees and others for facility clearance.
- 95.17 Processing facility clearance.
- 95.18 Key personnel.
- 95.19 Changes to security practices and procedures.
- 95.20 Grant, denial or termination of facility clearance.
- 95.21 Withdrawal of requests for facility clearance.
- 95.23 Termination of facility clearance.
- 95.25 Protection of classified information in storage.
- 95.27 Protection while in use.
- 95.29 Establishment of Restricted or Closed areas.
- 95.31 Protective personnel.
- 95.33 Security education.

## CONTROL OF INFORMATION

- 95.35 Access to matter classified as National Security Information and Restricted Data.
- 95.36 Access by representatives of the International Atomic Energy Agency or by participants in other international agreements.
- 95.37 Classification and preparation of documents.
- 95.39 External transmission of documents and material.
- 95.41 External receipt and dispatch records.
- 95.43 Authority to reproduce.
- 95.45 Changes in classification.
- 95.47 Destruction of matter containing classified information.
- 95.49 Security of automatic data processing (ADP) systems.
- 95.51 Retrieval of classified matter following suspension or revocation of access authorization.
- 95.53 Termination of facility clearance.
- 95.55 Continued applicability of the regulations in this part.
- 95.57 Reports.
- 95.59 Inspections.

## VIOLATIONS

- 95.61 Violations.
- 95.63 Criminal penalties.

AUTHORITY: Secs. 145, 161, 193, 68 Stat. 942, 948, as amended (42 U.S.C. 2165, 2201); sec. 201, 88 Stat. 1242, as amended (42 U.S.C. 5841); E.O. 10865, as amended, 3 CFR 1959-1963 COMP., p. 398 (50 U.S.C. 401, note); E.O. 12829, 3 CFR, 1993 Comp., p. 570; E.O. 12958, as amended, 3 CFR, 1995 Comp., p. 333; E.O. 12968, 3 CFR, 1995 Comp., p. 391.

SOURCE: 45 FR 14483, Mar. 5, 1980, unless otherwise noted.

## GENERAL PROVISIONS

### **§ 95.1 Purpose.**

The regulations in this part establish procedures for obtaining security facility approval and for safeguarding Secret and Confidential National Security Information and Restricted Data received or developed in conjunction with activities licensed, certified or regulated by the Commission. This part does not apply to Top Secret information because Top Secret information may not be forwarded to licensees, certificate holders, or others within the scope of an NRC license or certificate.

[62 FR 17690, Apr. 11, 1997]

### **§ 95.3 Scope.**

The regulations in this part apply to licensees, certificate holders and others regulated by the Commission who may require access to classified National Security Information and/or Restricted Data and/or Formerly Restricted Data (FRD) that is used, processed, stored, reproduced, transmitted, transported, or handled in connection with a license or certificate or an application for a license or certificate.

[62 FR 17690, Apr. 11, 1997]

### **§ 95.5 Definitions.**

*Access authorization* means an administrative determination that an individual (including a consultant) who is employed by or an applicant for employment with the NRC, NRC contractors, agents, licensees and certificate holders, or other persons designated by the Executive Director for Operations, is eligible for a security clearance for access to classified information.

*Act* means the Atomic Energy Act of 1954 (68 Stat. 919), as amended.

*Classified mail address* means a mail address established for each facility approved by the NRC, to which all classified information for the facility is to be sent.

*Classified matter* means documents or material containing classified information.

*Classified National Security Information* means information that has been determined pursuant to E.O. 12958 or any predecessor order to require protection against unauthorized disclosure and that is so designated.

*Classified shipping address* means an address established for a facility, approved by the NRC to which classified material that cannot be transmitted as normal mail is to be sent.

*Closed area* means an area that meets the requirements of the CSA, for the purpose of safeguarding classified material that, because of its size, nature, or operational necessity, cannot be adequately protected by the normal safeguards or stored during nonworking hours in approved containers.

*Cognizant Security Agency (CSA)* means agencies of the Executive Branch that have been authorized by E.O. 12829 to establish an industrial security program for the purpose of safeguarding classified information under the jurisdiction of those agencies when disclosed or released or released to U.S. industry. These agencies are the Department of Defense, the department of Energy, the Central Intelligence Agency, and the Nuclear Regulatory Commission. A facility has a CSA which exercises primary authority for the protection of classified information at the facility. The CSA for the facility provides security representation for other government agencies with security interests at the facility. The Secretary of Defense has been as Executive Agent for the National Industrial Security Program.

*Combination lock* means a three position, manipulation resistant, dial type lock bearing an Underwriters' Laboratories, Inc. certification that it is a Group 1 or Group IR unit.

*Commission* means the Nuclear Regulatory Commission or its duly authorized representatives.

*Facility (Security) Clearance (FCL)* means an administrative determination that, from a security viewpoint, a facility is eligible for access to classified information of a certain category (and all lower categories).

*Foreign ownership, control, or influence (FOCI)* means a foreign interest that has the power, direct or indirect, whether or not exercised, and whether or not exercisable through the ownership of a U.S. company's securities, by contractual arrangements or other means, to direct or decide matters affecting the management or operations of that company in a manner which may result in unauthorized access to classified information or may affect adversely the performance of classified contracts.

*Infraction* means any knowing, willful, or negligent action contrary to the requirements of E.O. 12958, or its implementing directives, that does not comprise a "violation," as defined in this section.

*Intrusion alarm* means a tamper-indicating electrical, electro-mechanical, electro-optical, electronic or similar device which will detect unauthorized intrusion by an individual into a building, protected area, security area, vital area, or material access area, and alert guards or watchmen by means of actuated visible and audible signals.

*License* means a license issued pursuant to 10 CFR parts 50, 70, or 72.

*Material* means chemical substance without regard to form; fabricated or processed item; or assembly, machinery or equipment.

*Matter* means documents or material.

*National security* means the national defense or foreign relations of the United States.

*Need-to-know* means a determination made by an authorized holder of classified information that a prospective recipient requires access to specific classified information in order to perform or assist in a lawful and authorized governmental function under the cognizance of the Commission.

*NRC "L" access authorization* means an access authorization granted by the Commission which is normally based on a national agency check and credit investigation (NAC&C) or national

agency check, inquiries and credit investigation (NACIC) conducted by the Office of Personnel Management.

*NRC "Q" access authorization* means an access authorization granted by the Commission based on a full field investigation conducted by the Office of Personnel Management, the Federal Bureau of Investigation, or other U.S. Government agency which conducts personnel security investigations.

*Person* means (1) any individual, corporation, partnership, firm, association, trust, estate, public or private institution, group, government agency other than the Commission or the Department of Energy (DOE), except that the DOE shall be considered a person to the extent that its facilities are subject to the licensing and related regulatory authority of the Commission pursuant to section 202 of the Energy Reorganization Act of 1974 and sections 104, 105 and 202 of the Uranium Mill Tailings Radiation Control Act of 1978, any State or any political subdivision of, or any political entity within a State, any foreign government or nation or any political subdivision of any such government or nation, or other entity; and (2) any legal successor, representative, agent or agency of the foregoing.

*Protective personnel* means guards or watchmen as defined in 10 CFR part 73 or other persons designated responsibility for the protection of classified matter.

*Restricted area* means a controlled access area established to safeguard classified material, that, because of its size or nature, cannot be adequately protected during working hours by the usual safeguards, but that is capable of being stored during non-working hours in an approved repository or secured by other methods approved by the CSA.

*Restricted data* means all data concerning design, manufacture or utilization of atomic weapons, the production of special nuclear material, or the use of special nuclear material in the production of energy, but shall not include data declassified or removed from the Restricted Data category pursuant to section 142 of the Act.

*Security area* means a physically defined space containing classified mat-

ter and subject to physical protection and personnel access controls.

*Security container* includes any of the following repositories: (1) A security filing cabinet—one that bears a Test Certification Label on the side of the locking drawer, inside wall adjacent to the locking drawer, or interior door plate, and is marked, *General Services Administration Approved Security Container* on the exterior of the top drawer or door.

(2) A safe—burglar-resistive cabinet or chest which bears a label of the Underwriters' Laboratories, Inc. certifying the unit to be a TL-15, TL-30, or TRTL-30, and has a body fabricated of not less than 1 inch steel and a door fabricated of not less than 1½ inches steel exclusive of the combination lock and bolt work; or bears a Test Certification Label on the inside of the door and is marked *General Services Administration Approved Security Container* and has a body of steel at least ½" thick, and a combination locked steel door at least 1" thick, exclusive of bolt work and locking devices.

(3) A vault—a windowless enclosure constructed with walls, floor, roof and door(s) that will delay penetration sufficient to enable the arrival of emergency response forces capable of preventing theft, diversion, damage or compromise of classified information or matter, when delay time is assessed in conjunction with detection and communication subsystems of the physical protection system.

(4) A vault-type room—a room which has a combination lock door and is protected by an intrusion alarm system which alarms upon the unauthorized penetration of a person anywhere into the room.

(5) Other repositories which in the judgment of the Division of Security would provide comparable physical protection.

*Security facility*—any facility which has been approved by NRC for using, processing, storing, reproducing, transmitting or handling classified matter.

*Security reviews* means aperiodic security reviews of cleared facilities conducted to ensure that safeguards employed by licensees and others are adequate for the protection of classified information.

*Supplemental protection* means additional security procedures such as intrusion detection systems, security guards, and access control systems.

*Violation* means any knowing, willful, or negligent action that could reasonably be expected to result in an unauthorized disclosure of classified information or any knowing, willful, or negligent action to classify or continue the classification of information contrary to the requirements of E.O. 12958 or its implementing directives.

[45 FR 14483, Mar. 5, 1980, as amended at 46 FR 58284, Dec. 1, 1981; 47 FR 38683, Sept. 2, 1982; 48 FR 24320, June 1, 1983; 50 FR 36984, Sept. 11, 1985; 55 FR 11575, Mar. 29, 1990; 55 FR 14379, Apr. 17, 1990; 59 FR 48974, Sept. 23, 1994; 62 FR 17691, Apr. 11, 1997]

#### § 95.7 Interpretations.

Except as specifically authorized by the Commission in writing, no interpretation of the meaning of the regulations in this part by any officer or employee of the Commission other than a written interpretation by the General Counsel will be recognized to be binding upon the Commission.

#### § 95.8 Information collection requirements: OMB approval.

(a) The Nuclear Regulatory Commission has submitted the information collection requirements contained in this part to the Office of Management and Budget (OMB) for approval as required by the Paperwork Reduction Act (44 U.S.C. 3501 et seq.). The NRC may not conduct or sponsor, and a person is not required to respond to, a collection of information unless it displays a currently valid OMB control number. OMB has approved the information collection requirements contained in this part under control number 3150-0047.

(b) The approved information collection requirements contained in this part appear in §§ 95.11, 95.15, 95.18, 95.21, 95.25, 95.33, 95.36, 95.37, 95.41, 95.45, 95.47, 95.53, and 95.57.

[62 FR 52190, Oct. 6, 1997]

#### § 95.9 Communications.

Except where otherwise specified, all communications and reports concerning the regulations in this part should be addressed to the Director, Division

of Security, Nuclear Regulatory Commission, Washington, DC 20555.

#### § 95.11 Specific exemptions.

The Commission may, upon application of any interested party, grant an exemption from the requirements of part 95. Exemptions will be granted only if they are authorized by law and will not constitute an undue risk to the common defense and security. The licensee shall retain the documentation related to the request, notification, and processing of an exemption for three years beyond the period covered by the exemption.

[53 FR 19263, May 27, 1988]

#### § 95.13 Maintenance of records.

(a) Each licensee, certificate holder or other person granted facility clearance under this part shall maintain records as prescribed within the part. These records are subject to review and inspection by CSA representatives during security reviews.

(b) Each record required by this part must be legible throughout the retention period specified by each Commission regulation. The record may be the original or a reproduced copy or a microform provided that the copy or microform is authenticated by authorized personnel and that the microform is capable of producing a clear copy throughout the required retention period. The record may also be stored in electronic media with the capability for producing legible, accurate, and complete records during the required retention period. Records such as letters, drawings, specifications, must include all pertinent information such as stamps, initials, and signatures. The licensee shall maintain adequate safeguards against tampering with and loss of records.

[53 FR 19263, May 27, 1988, as amended at 62 FR 17691, Apr. 11, 1997]

#### PHYSICAL SECURITY

#### § 95.15 Approval for processing licensees and others for facility clearance.

(a) A licensee, certificate holder or other person who has a need to use, process, store, reproduce, transmit,

transport, or handle NRC classified information at any location in connection with Commission related activities shall promptly request an NRC facility clearance. This specifically includes situations where a licensee, certificate holder or other person needs a contractor or consultant to have access to NRC classified information. However, it is not necessary for a licensee, certificate holder or other person to request an NRC facility clearance for access to another agency's classified information at that agency's facilities or to store that agency's classified information at their facility, provided no NRC classified information is involved and they meet the security requirements of the other agency. If NRC classified information is involved the requirements of § 95.17 apply.

(b) The request must include the name of the facility, the location of the facility and an identification of any facility clearance issued by another government agency. If there is no existing facility clearance, the request must include a security Standard Practice Procedures Plan that outlines the facility's proposed security procedures and controls for the protection of classified information, a floor plan of the area in which the matter is to be used, processed, stored, reproduced, transmitted, transported or handled; and Foreign Ownership, Control or Influence information.

(c) NRC will promptly inform applicants of the acceptability of the request for further processing and will notify the licensee or other person of their decision in writing.

[45 FR 14483, Mar. 5, 1980, as amended at 48 FR 24321, June 1, 1983; 50 FR 36984, Sept. 11, 1985; 59 FR 48974, Sept. 23, 1994; 62 FR 17691, Apr. 11, 1997]

#### **§ 95.17 Processing facility clearance.**

(a) Following the receipt of an acceptable request for facility clearance, the NRC will either accept an existing facility clearance granted by a current CSA and authorize possession of license or certificate related classified information or process the facility for a facility clearance. Processing will include—

(1) A determination based on review and approval of a Standard Practice

Procedure Plan that granting of the Facility Clearance would not be inconsistent with the national interest, including a finding that the facility is not under foreign ownership, control, or influence to such a degree that a termination could not be made;

(2) An acceptable security review conducted by the NRC;

(3) Submitting key management personnel for personnel clearances (PCLs); and

(4) Appointing a U.S. citizen employee as the facility security officer.

(b) An interim Facility Clearance may be granted by the CSA on a temporary basis pending completion of the full investigative requirements.

[62 FR 17692, Apr. 11, 1997]

#### **§ 95.18 Key personnel.**

The senior management official and the Facility Security Officer must always be cleared to a level commensurate with the Facility Clearance. Other key management officials, as determined by the CSA, must be granted an access authorization or be excluded from classified access. When formal exclusion action is required, the organization's board of directors or similar executive body shall affirm the following, as appropriate.

(a) Officers, directors, partners, regents, or trustees (designated by name) that are excluded may not require, may not have, and can be effectively excluded from access to all classified information disclosed to the organization. These individuals also may not occupy positions that would enable them to adversely affect the organization's policies or practices in the performance of activities involving classified information. This action will be made a matter of record by the organization's executive body. A copy of the resolution must be furnished to the CSA.

(b) Officers, directors, partners, regents, or trustees (designated by name) that are excluded may not require, may not have, and can be effectively denied access to higher-level classified information (specify which higher level(s)). These individuals may not occupy positions that would enable them to adversely affect the organization's policies or practices in the protection

#### § 95.19

of classified information. This action will be made a matter of record by the organization's executive body. A copy of the resolution must be furnished to the CSA.

[62 FR 17692, Apr. 11, 1997]

#### **§95.19 Changes to security practices and procedures.**

(a) Except as specified in paragraph (b) of this section, each licensee, certificate holder or other person shall obtain prior CSA approval for any proposed change to the name, location, security procedures and controls, or floor plan of the approved facility. A written description of the proposed change must be furnished to the CSA with copies to the Director, Division of Security, office of Administration, NRC, Washington, DC 20555-0001 (if NRC is not the CSA), and the NRC Regional Administrator of the cognizant Regional Office listed in appendix A of part 73. The CSA shall promptly respond in writing to all such proposals. Some examples of substantive changes requiring prior CSA approval include—

(1) A change in the approved facility's classified mail address; or

(2) A temporary or permanent change in the location of the approved facility (e.g., moving or relocating NRC's classified interest from one room or building to another).

(b) A licensee or other person may effect a minor, non-substantive change to an approved Standard Practice Procedures Plan for the safeguarding of classified information without receiving prior CSA approval, provided prompt notification of such minor change is furnished to the addresses noted in paragraph (a) of this section, and the change does not decrease the effectiveness of the Standard Practice Procedures Plan. Some examples of minor, non-substantive changes to the Standard Practice Procedures Plan include—

(1) The designation/appointment of a new facility security officer; or

(2) A revision to protective personnel patrol routine, provided the new rou-

#### 10 CFR Ch. I (1–1–99 Edition)

tine continues to meet the minimum requirements of this part.

[50 FR 36984, Sept. 11, 1985, as amended at 52 FR 31613, Aug. 21, 1987; 54 FR 53316, Dec. 28, 1989. Redesignated and amended at 62 FR 17692, Apr. 11, 1997]

#### **§95.20 Grant, denial or termination of facility clearance.**

The Division of Security shall provide notification in writing (or orally with written confirmation) to the licensee or other organization, of the Commission's grant, acceptance of another agency's Facility Clearance, denial, or termination of facility clearance. This information shall also be furnished to representatives of the NRC, NRC licensees, NRC certificate holders, NRC contractors, or other Federal agencies having a need to transmit classified information to the licensee or other person.

[62 FR 17692, Apr. 11, 1997]

#### **§95.21 Withdrawal of requests for facility clearance.**

When a request for facility clearance is to be withdrawn or canceled, the requester shall notify the NRC Division of Security immediately by telephone so that processing for this approval may be terminated. The notification must identify the full name of the individual requesting discontinuance, his position with the facility, and the full identification of the facility. The requestor shall confirm the telephone notification promptly in writing.

[62 FR 17692, Apr. 11, 1997]

#### **§95.23 Termination of facility clearance.**

(a) Facility clearance will be terminated when—

(1) There is no longer a need to use, process, store, reproduce, transmit, transport or handle classified matter at the facility; or

(2) The Commission makes a determination that continued facility clearance is not in the interest of national security.

(b) When facility clearance is terminated, the licensee or other person will

be notified in writing of the determination and the procedures outlined in § 95.53 apply.

[62 FR 17692, Apr. 11, 1997]

**§ 95.25 Protection of classified information in storage.**

(a) Secret documents, while unattended or not in actual use, must be stored in—

(1) A safe, steel file cabinet, or safe-type steel file container that has an automatic unit locking mechanism. All such receptacles will be accorded supplemental protection during non-working hours; or

(2) Any steel file cabinet that has four sides and a top and bottom (all permanently attached by welding, rivets or peened bolts so the contents cannot be removed without leaving visible evidence of entry) and is secured by a rigid metal lock bar and an approved key operated or combination padlock. The keepers of the rigid metal lock bar must be secured to the cabinet by welding, rivets, or bolts, so they cannot be removed and replaced without leaving evidence of the entry. The drawers of the container must be held securely, so their contents cannot be removed without forcing open the drawer. This type cabinet will be accorded supplemental protection during non-working hours.

(b) Confidential matter while unattended or not in use must be stored in the same manner as SECRET matter except that no supplemental protection is required.

(c) Classified lock combinations.

(1) A minimum number of authorized persons may know the combinations to authorized storage containers. Security containers, vaults, cabinets, and other authorized storage containers must be kept locked when not under the direct supervision of an authorized person entrusted with the contents.

(2) Combinations must be changed by a person authorized access to the contents of the container, or by the Facility Security Officer or his or her designee. Combinations must be changed upon—

(i) The initial use of an approved container or lock for the protection of classified material;

(ii) The termination of employment of any person having knowledge of the

combination, or when the clearance granted to any such person has been withdrawn, suspended, or revoked;

(iii) The compromise or suspected compromise of a container or its combination, or discovery of a container left unlocked and unattended; or

(iv) At other times when considered necessary by the Facility Security Officer or CSA.

(d) Records of combinations. If a record is made of a combination, the record must be marked with the highest classification of material authorized for storage in the container. Superseded combinations must be destroyed.

(e) *Selections of combinations.* Each combination must be randomly selected and require the use of at least three different numbers. In selecting combinations, multiples, simple arithmetical ascending or descending series, telephone numbers, social security numbers, car license numbers, and calendar dates such as birthdates and anniversaries, shall be avoided.

(f) *Cautions regarding combinations.* (1) When closing a combination lock, the dial must be turned at least four times in the same direction.

(2) Combinations shall be changed only by persons authorized access to Secret or Confidential National Security Information and/or Restricted Data depending upon the matter authorized to be stored in the security container.

(g) Posted information. Containers may not bear external markings indicating the level of classified material authorized for storage. A record of the names of persons having knowledge of the combination must be posted inside the container.

(h) End of day security checks.

(1) Facilities that store classified material shall establish a system of security checks at the close of each working day to ensure that all classified material and security repositories have been appropriately secured.

(2) Facilities operating with multiple work shifts shall perform the security checks at the end of the last working shift in which classified material had been removed from storage for use. The checks are not required during continuous 24-hour operations.

(i) Unattended security container found opened. If an unattended security container housing classified matter is found unlocked, the custodian or an alternate must be notified immediately. The container must be secured by protective personnel and the contents inventoried as soon as possible but not later than the next workday. A report reflecting all actions taken must be submitted to the responsible Regional Office (see appendix A, 10 CFR part 73 for addresses) with an information copy to the NRC Division of Security. The licensee shall retain records pertaining to these matters for three years after completion of final corrective action.

(j) Supervision of keys and padlocks. Use of key-operated padlocks are subject to the following requirements:

(1) A key and lock custodian shall be appointed to ensure proper custody and handling of keys and locks used for protection of classified material;

(2) A key and lock control register must be maintained to identify keys for each lock and their current location and custody;

(3) Keys and locks must be audited each month;

(4) Keys must be inventoried with each change of custody;

(5) Keys must not be removed from the premises;

(6) Keys and spare locks must be protected equivalent to the level of classified material involved;

(7) Locks must be changed or rotated at least annually, and must be replaced after loss or compromise of their operable keys; and

(8) Master keys may not be made.

[45 FR 14483, Mar. 5, 1980, as amended at 47 FR 9196, Mar. 4, 1982; 50 FR 36985, Sept. 11, 1985; 53 FR 19263, May 27, 1988; 59 FR 48975, Sept. 23, 1994; 62 FR 17693, Apr. 11, 1997]

#### § 95.27 Protection while in use.

While in use, matter containing classified information must be under the direct control of an authorized individual to preclude physical, audio and visual access by persons who do not have the prescribed access authorization or other written CSA disclosure authorization (see § 95.36 for additional information concerning authorizations).

[62 FR 17693, Apr. 11, 1997]

#### § 95.29 Establishment of Restricted or Closed areas.

(a) If, because of its nature, sensitivity or importance, matter containing classified information cannot otherwise be effectively controlled in accordance with the provisions of §§ 95.25 and 95.27, a Restricted or Closed Area must be established to protect such matter.

(b) The following measures apply to Restricted Areas:

(1) Restricted areas must be separated from adjacent areas by a physical barrier designed to prevent unauthorized access (physical, audio, and visual) into these areas.

(2) Controls must be established to prevent unauthorized access to and removal of classified matter.

(3) Access to classified matter must be limited to persons who possess appropriate access authorization or other written CSA disclosure authorization and who require access in the performance of their official duties or regulatory obligations.

(4) Persons without appropriate access authorization for the area visited must be escorted by an appropriate CSA access authorized person at all times while within Restricted or Closed Areas.

(5) Each individual authorized to enter a Restricted or Closed Area must be issued a distinctive form of identification (e.g., badge) when the number of employees assigned to the area exceeds thirty per shift.

(6) During nonworking hours, admittance must be controlled by protective personnel. Protective personnel shall conduct patrols during nonworking hours at least every 8 hours and more frequently if necessary to maintain a commensurate level of protection. Entrances must be continuously monitored by protective personnel or by an approved alarm system.

(c) Due to the size and nature of the classified material, or operational necessity, it may be necessary to construct Closed Areas for storage because GSA-approved containers or vaults are unsuitable or impractical. Closed Areas must be approved by the CSA. The following measures apply to Closed Areas:



## Nuclear Regulatory Commission

## § 95.33

(1) Access to Closed Areas must be controlled to preclude unauthorized access. This may be accomplished through the use of a cleared employee or by a CSA approved access control device or system.

(2) Access must be limited to authorized persons who have an appropriate security clearance and a need-to-know for the classified material/information within the area. Persons without the appropriate level of clearance and/or need-to-know must be escorted at all times by an authorized person where inadvertent or unauthorized exposure to classified information cannot otherwise be effectively prevented.

(3) The Closed Area must be accorded supplemental protection during non-working hours. During these hours, admittance to the area must be controlled by locked entrances and exits secured by either an approved built-in combination lock or an approved combination or key-operated padlock. However, doors secured from the inside with a panic bolt (for example, actuated by a panic bar), a dead bolt, a rigid wood or metal bar, or other means approved by the CSA, do not require additional locking devices.

(4) Open shelf or bin storage of classified documents in Closed Areas requires CSA approval. Only areas protected by an approved intrusion detection system will qualify for approval.

[62 FR 17693, Apr. 11, 1997]

### § 95.31 Protective personnel.

Whenever protective personnel are used to protect classified information they shall:

(a) Possess an "L" access authorization (or CSA equivalent) if the licensee or other person possesses information classified Confidential National Security Information, Confidential Restricted Data or Secret National Security Information.

(b) Possess a "Q" access authorization (or CSA equivalent) if the licensee or other person possesses Secret Restricted Data related to nuclear weapons design, manufacturing and vulnerability information; and certain particularly sensitive Naval nuclear Propulsion Program Information (e.g., fuel manufacturing technology) and the

protective personnel require access as part of their regular duties.

[62 FR 17694, Apr. 11, 1997]

### § 95.33 Security education.

All cleared employees must be provided with security training and briefings commensurate with their involvement with classified information. The facility may obtain defensive security, threat awareness, and other education and training information and material from their CSA or other sources.

(a) Facility Security Officer Training. Licensees and others are responsible for ensuring that the Facility Security Officer, and others performing security duties, complete security training deemed appropriate by the CSA. Training requirements must be based on the facility's involvement with classified information and may include a Facility Security Officer orientation course and, for Facility Security Officers at facilities with safeguarding capability, a Facility Security Officer Program Management Course. Training, if required, should be completed within 1 year of appointment to the position of Facility Security Officer.

(b) Government-Provided Briefings. The CSA is responsible for providing initial security briefings to the Facility Security Officer, and for ensuring that other briefings required for special categories of information are provided.

(c) Temporary Help Suppliers. A temporary help supplier, or other contractor who employs cleared individuals solely for dispatch elsewhere, is responsible for ensuring that required briefings are provided to their cleared personnel. The temporary help supplier or the using licensee or other facility may conduct these briefings.

(d) Classified Information Nondisclosure Agreement (SF-312). The SF-312 is an agreement between the United States and an individual who is cleared for access to classified information. An employee issued an initial access authorization must, in accordance with the requirements of § 25.23 of this chapter, execute an SF-312 before being granted access to classified information. The Facility Security Officer shall forward the executed SF-312 to the CSA for retention. If the employee

refuses to execute the SF-312, the licensee or other facility shall deny the employee access to classified information and submit a report to the CSA. The SF-312 must be signed and dated by the employee and witnessed. The employee's and witness' signatures must bear the same date.

(e) Initial Security Briefings. Before being granted access to classified information, an employee shall receive an initial security briefing that includes the following topics:

- (1) A Threat Awareness Briefing.
- (2) A Defensive Security Briefing.
- (3) An overview of the security classification system.

(4) Employee reporting obligations and requirements.

(5) Security procedures and duties applicable to the employee's job.

(f) Refresher Briefings. The licensee or other facility shall conduct periodic refresher briefings for all cleared employees. As a minimum, the refresher briefing must reinforce the information provided during the initial briefing and inform employees of appropriate changes in security regulations. This requirement may be satisfied by use of audio/video materials and by issuing written materials on a regular basis.

(g) Debriefings. Licensee and other facilities shall debrief cleared employees at the time of termination of employment (discharge, resignation, or retirement); when an employee's access authorization is terminated, suspended, or revoked; and upon termination of the Facility Clearance.

(h) Records reflecting an individual's initial and refresher security orientations and security termination must be maintained for three years after termination of the individual's access authorization.

[62 FR 17694, Apr. 11, 1997]

#### CONTROL OF INFORMATION

### **§95.35 Access to matter classified as National Security Information and Restricted Data.**

(a) Except as the Commission may authorize, no person subject to the regulations in this part may receive or may permit any individual to have access to matter revealing Secret or Con-

fidential National Security Information or Restricted Data unless the individual has:

(1)(i) A "Q" access authorization which permits access to matter classified as Secret and Confidential Restricted Data or Secret and Confidential National Security Information which includes intelligence information, CRYPTO (i.e., cryptographic information) or other classified communications security (COMSEC) information, or

(ii) An "L" access authorization which permits access to matter classified as Confidential Restricted Data and Secret and Confidential National Security Information other than that noted in paragraph (a)(1)(i) of this section except that access to certain Confidential COMSEC information is permitted as authorized by a National Communications Security Committee waiver dated February 14, 1984.

(2) An established "need-to-know" for the matter (See Definitions, §95.5).

(3) NRC-approved storage facilities if classified documents or material are to be transmitted to the individual.

(b) Matter classified as National Security Information or Restricted Data shall not be released by a licensee or other person subject to part 95 to any personnel other than properly access authorized Commission licensee employees, or other individuals authorized access by the Commission.

(c) Access to matter which is National Security Information at NRC-licensed facilities or NRC-certified facilities by authorized representatives of IAEA is permitted in accordance with §95.36.

[59 FR 48975, Sept. 23, 1994]

### **§95.36 Access by representatives of the International Atomic Energy Agency or by participants in other international agreements.**

(a) Based upon written disclosure authorization from the NRC Division of Security that an individual is an authorized representative of the International Atomic Energy Agency (IAEA) or other international organization and that the individual is authorized to make visits or inspections in

accordance with an established agreement with the United States Government, a licensee, certificate holder or other person subject to this part shall permit the individual (upon presentation of the credentials specified in § 75.7 of this chapter and any other credentials identified in the disclosure authorization) to have access to matter which is classified National Security Information that is relevant to the conduct of a visit or inspection. A disclosure authorization under this section does not authorize a licensee, certificate holder, or other person subject to this part to provide access to Restricted Data.

(b) For purposes of this section, classified National Security Information is relevant to the conduct of a visit or inspection if—

(1) In the case of a visit, this information is needed to verify information according to § 75.13 of this chapter; or

(2) In the case of an inspection, an inspector is entitled to have access to the information under § 75.42 of this chapter.

(c) In accordance with the specific disclosure authorization provided by the Division of Security, licensees or other persons subject to this part are authorized to release (i.e., transfer possession of) copies of documents which contain classified National Security Information directly to IAEA inspectors and other representatives officially designated to request and receive classified National Security Information documents. These documents must be marked specifically for release to IAEA or other international organizations in accordance with instructions contained in the NRC's disclosure authorization letter. Licensees and other persons subject to this part may also forward these documents through the NRC to the international organization's headquarters in accordance with the NRC disclosure authorization. Licensees and other persons may not reproduce documents containing classified National Security Information except as provided in § 95.43.

(d) Records regarding these visits and inspections must be maintained for five years beyond the date of the visit or inspection. These records must specifically identify each document which

has been released to an authorized representative and indicate the date of the release. These records must also identify (in such detail as the Division of Security, by letter, may require) the categories of documents that the authorized representative has had access and the date of this access. A licensee or other person subject to this part shall also retain Division of Security disclosure authorizations for five years beyond the date of any visit or inspection when access to classified information was permitted.

(e) Licensees or other persons subject to this part shall take such measures as may be necessary to preclude access to classified matter by participants of other international agreements unless specifically provided for under the terms of a specific agreement.

[62 FR 17694, Apr. 11, 1997]

#### **§ 95.37 Classification and preparation of documents.**

(a) Classification. Classified information generated or possessed by a licensee or other person must be appropriately marked. Classified material which is not conducive to markings (e.g., equipment) may be exempt from this requirement. These exemptions are subject to the approval of the CSA on a case-by-case basis. If a person or facility generates or possesses information that is believed to be classified based on guidance provided by the NRC or by derivation from classified documents, but which no authorized classifier has determined to be classified, the information must be protected and marked with the appropriate classification markings pending review and signature of an NRC authorized classifier. This information shall be protected as classified information pending final determination.

(b) Classification consistent with content. Each document containing classified information shall be classified Secret or Confidential according to its content. NRC licensees or others subject to the requirements of 10 CFR Part 95 may not make original classification decisions.

(c) Markings required on face of documents.

(1) For derivative classification of classified National Security Information:

(i) Derivative classifications of classified National Security Information must contain the identity of the source document or the classification guide, including the agency and office of origin, on the “Derived From” line and its classification date. If more than one source is cited, the “Derived From” line should indicate “Multiple Sources.”

(ii) Declassification instructions. When marking derivatively classified documents, the “DECLASSIFY ON” line must carry forward the declassification instructions as reflected in the original document. If multiple sources are used, the instructions will carry forward the longest duration.

(iii) If the source document used for derivative classification contains the declassification instruction, “Originating Agency’s Determination Required” (OADR), the new document should reflect the date of the original classification of the information as contained in the source document or classification guide. An example of the stamp might be as follows:

Derived From \_\_\_\_\_  
(Source)  
Reason \_\_\_\_\_  
Declassify On: *Source Marked* “OADR”  
Date of Source: \_\_\_\_\_  
Classifier: \_\_\_\_\_  
(Name/Title/Number)

(iv) The derivative classifier shall maintain the identification of each source with the file or record copy of the derivatively classified document.

(2) For Restricted Data documents:

(i) Identity of the classifier. The identity of the classifier must be shown by completion of the “Derivative Classifier” line. The “Derivative Classifier” line must show the name of the person classifying the document and the basis for the classification. Dates for downgrading or declassification do not apply.

(ii) Classification designation (e.g., Secret, Confidential) and Restricted Data. NOTE: No “Declassification” instructions will be placed on documents containing Restricted Data.

(d) Placement of markings. The highest classification marking assigned to

a document must be placed in a conspicuous fashion in letters at the top and bottom of the outside of the front covers and title pages, if any, and first and last pages on which text appears, on both bound and unbound documents, and on the outside of back covers of bound documents. The balance of the pages must be marked at the top and bottom with:

(1) The overall classification marking assigned to the document;

(2) The highest classification marking required by content of the page; or

(3) The marking UNCLASSIFIED if they have no classified content.

(e) Additional markings.

(1) If the document contains any form of Restricted Data, it must bear the appropriate marking on the first page of text, on the front cover and title page, if any. For example: “This document contains Restricted Data as defined in the Atomic Energy Act of 1954. Unauthorized disclosure subject to Administrative and Criminal Sanctions.”

(2) Limitation on reproduction or dissemination. If the originator or classifier determines that reproduction or further dissemination of a document should be restricted, the following additional wording may be placed on the face of the document:

Reproduction or Further Dissemination Requires Approval of \_\_\_\_\_

If any portion of this additional marking does not apply, it should be crossed out.

(f) Portion markings. In addition to the information required on the face of the document, each classified document is required, by marking or other means, to indicate clearly which portions are classified (e.g., paragraphs or pages) and which portions are not classified. The symbols (S) for Secret, (C) for Confidential, (U) for Unclassified, or (RD) for Restricted Data may be used immediately preceding or following the text to which it applies, except that the designation must follow titles or subjects. (Portion marking of paragraphs is not required for documents containing Restricted Data.) If this type of portion marking is not practicable, the document must contain a description sufficient to identify the

## Nuclear Regulatory Commission

## § 95.39

classified information and the unclassified information.

### Example

Pages 1-3 Secret  
Pages 4-19 Unclassified  
Pages 20-26 Secret  
Pages 27-32 Confidential

(g) Transmittal document. If a document transmitting classified information contains no classified information or the classification level of the transmittal document is not as high as the highest classification level of its enclosures, then the document must be marked at the top and bottom with a classification at least as high as its highest classified enclosure. The classification may be higher if the enclosures, when combined, warrant a higher classification than any individual enclosure. When the contents of the transmittal document warrants a lower classification than the highest classified enclosure(s) or combination of enclosures or requires no classification, a stamp or marking such as the following must also be used on the transmittal document:

UPON REMOVAL OF ATTACHMENTS THIS DOCUMENT IS:

(Classification level of transmittal document standing alone or the word "UNCLASSIFIED" if the transmittal document contains no classified information.)

(h) Classification challenges. Persons in authorized possession of classified National Security Information who in good faith believe that the information's classification status (i.e. that the document), is classified at either too high a level for its content (overclassification) or too low for its content (underclassification) are expected to challenge its classification status. Persons who wish to challenge a classification status shall—

(1) Refer the document or information to the originator or to an authorized NRC classifier for review. The authorized classifier shall review the document and render a written classification decision to the holder of the information.

(2) In the event of a question regarding classification review, the holder of the information or the authorized classifier shall consult the NRC Division of

Security, Information Security Branch, for assistance.

(3) Persons who challenge classification decisions have the right to appeal the classification decision to the Interagency Security Classification Appeals Panel.

(4) Persons seeking to challenge the classification of information will not be the subject of retribution.

(i) Files, folders or group of documents. Files, folders, binders, or groups of physically connected documents must be marked at least as high as the highest classified document which they contain.

(j) Drafts and working papers. Drafts of documents and working papers which contain, or which are believed to contain, classified information must be marked as classified information.

(k) Classification guidance. Licensees, certificate holders, or other persons subject to this part shall classify and mark classified matter as National Security Information or Restricted Data, as appropriate, in accordance with classification guidance provided by the NRC as part of the facility clearance process.

[62 FR 17695, Apr. 11, 1997]

### § 95.39 External transmission of documents and material.

(a) Restrictions. Documents and material containing classified information received or originated in connection with an NRC license or certificate must be transmitted only to CSA approved security facilities.

(b) Preparation of documents. Documents containing classified information must be prepared in accordance with the following when transmitted outside an individual installation.

(1) The documents must be enclosed in two sealed opaque envelopes or wrappers.

(2) The inner envelope or wrapper must contain the addressee's classified mail address and the name of the intended recipient. The appropriate classification must be placed on both sides of the envelope (top and bottom) and the additional markings, as appropriate, referred to in § 95.37(e) must be placed on the side bearing the address.

(3) The outer envelope or wrapper must contain the addressee's classified

mail address. The outer envelope or wrapper may not contain any classification, additional marking or other notation that indicates that the enclosed document contains classified information.

(4) A receipt that contains an unclassified description of the document, the document number, if any, date of the document, classification, the date of transfer, the recipient and the person transferring the document must be enclosed within the inner envelope containing the document and be signed by the recipient and returned to the sender whenever the custody of a Secret document is transferred. This receipt process is at the option of the sender for Confidential information.

(c) Methods of transportation.

(1) Secret matter may be transported only by one of the following methods within and directly between the U.S., Puerto Rico, or a U.S. possession or trust territory:

(i) U.S. Postal Service Express Mail and U.S. Postal Service Registered Mail.

NOTE: The "Waiver of Signature and Indemnity" block on the U.S. Postal Service Express Mail Label 11-B may not be executed and the use of external (street side) express mail collection boxes is prohibited.

(ii) A cleared "Commercial Carrier."

(iii) A cleared commercial messenger service engaged in the intracity/local area delivery (same day delivery only) of classified material.

(iv) A commercial delivery company, approved by the CSA, that provides nationwide, overnight service with computer tracing and reporting features. These companies need not be security cleared.

(v) Other methods as directed, in writing, by the CSA.

(2) Confidential matter may be transported by one of the methods set forth in paragraph (c)(1) of this section, by U.S. first class, express or certified mail. First class, express, or certified mail may be used in transmission of Confidential documents to Puerto Rico or any United States territory or possession.

(d) Telecommunication of classified information. Classified information may not be telecommunicated unless the telecommunication system has

been approved by the CSA. Licensees, certificate holders or other persons who may require a secure telecommunication system shall submit a telecommunication plan as part of their request for facility clearance, as outlined in § 95.15, or as an amendment to their existing Standard Practice Procedures Plan for the protection of classified information.

(e) Security of classified information in transit. Classified matter that, because of its nature, cannot be transported in accordance with § 95.39(c), may only be transported in accordance with procedures approved by the CSA. Procedures for transporting classified matter are based on a satisfactory transportation plan submitted as part of the licensee's, certificate holder, or other person's request for facility clearance or submitted as an amendment to its existing Standard Practice Procedures Plan.

[62 FR 17696, Apr. 11, 1997]

#### **§ 95.41 External receipt and dispatch records.**

Each licensee, certificate holder or other person possessing classified information shall maintain a record that reflects:

- (a) The date of the material;
- (b) The date of receipt or dispatch;
- (c) The classification;
- (d) An unclassified description of the material; and
- (e) The identity of the sender from which the material was received or recipient to which the material was dispatched. receipt and dispatch records must be retained for 2 years.

[62 FR 17697, Apr. 11, 1997]

#### **§ 95.43 Authority to reproduce.**

(a) Each licensee or other person possessing classified information shall establish a reproduction control system to ensure that reproduction of classified material is held to the minimum consistent with operational requirements. Classified reproduction must be accomplished by authorized employees knowledgeable of the procedures for classified reproduction. The use of technology that prevents, discourages,

## Nuclear Regulatory Commission

## § 95.51

or detects the unauthorized reproduction of classified documents is encouraged.

(b) Unless restricted by the CSA, Secret and Confidential documents may be reproduced. Reproduced copies of classified documents are subject to the same protection as the original documents.

(c) All reproductions of classified material must be conspicuously marked with the same classification markings as the material being reproduced. Copies of classified material must be reviewed after the reproduction process to ensure that these markings are visible.

[62 FR 17697, Apr. 11, 1997]

### § 95.45 Changes in classification.

(a) Documents containing classified National Security Information must be downgraded or declassified as authorized by the NRC classification guides or as determined by the NRC. Requests for downgrading or declassifying any NRC classified information should be forwarded to the NRC Division of Security, Office of Administration, Washington, DC 20555-0001. Requests for downgrading or declassifying of Restricted Data will be forwarded to the NRC Division of Security for coordination with the Department of Energy.

(b) If a change of classification or declassification is approved, the previous classification marking must be canceled and the following statement, properly completed, must be placed on the first page of the document:

Classification canceled (or changed to)

---

(Insert appropriate classification)  
By authority of

---

(Person authorizing change in classification)  
By

---

(Signature of person making change and date thereof)

(c) New markings reflecting the current classification status of the document will be applied in accordance with the requirements of § 95.37.

(d) Any persons making a change in classification or receiving notice of such a change shall forward notice of

the change in classification to holders of all copies as shown on their records.

[62 FR 17697, Apr. 11, 1997]

### § 95.47 Destruction of matter containing classified information.

Documents containing classified information may be destroyed by burning, pulping, or another method that ensures complete destruction of the information that they contain. The method of destruction must preclude recognition or reconstruction of the classified information. Any doubts on methods should be referred to the CSA. If the document contains Secret information, a record of the subject or title, document number, if any, originator, its date of origination and the date of destruction must be signed by the person destroying the document and must be maintained in the office of the custodian at the time of destruction. These destruction records must be retained for two years after destruction.

[62 FR 17697, Apr. 11, 1997]

### § 95.49 Security of automatic data processing (ADP) systems.

Classified data or information may not be processed or produced on an ADP system unless the system and procedures to protect the classified data or information have been approved by the CSA. Approval of the ADP system and procedures is based on a satisfactory ADP security proposal submitted as part of the licensee's or other person's request for facility clearance outlined in § 95.15 or submitted as an amendment to its existing Standard Practice Procedures Plan for the protection of classified information.

[62 FR 17697, Apr. 11, 1997]

### § 95.51 Retrieval of classified matter following suspension or revocation of access authorization.

In any case where the access authorization of an individual is suspended or revoked in accordance with the procedures set forth in part 25 of this chapter, or other relevant CSA procedures, the licensee, certificate holder or other organization shall, upon due notice

from the Commission of such suspension or revocation, retrieve all classified information possessed by the individual and take the action necessary to preclude that individual having further access to the information.

[62 FR 17697, Apr. 11, 1997]

**§95.53 Termination of facility clearance.**

(a) If the need to use, process, store, reproduce, transmit, transport, or handle classified matter no longer exists, the facility clearance will be terminated. The facility may deliver all documents and materials containing classified information to the Commission or to a person authorized to receive them or destroy all such documents and materials. In either case, the facility shall submit a certification of non-possession of classified information to the NRC Division of Security.

(b) In any instance where facility clearance has been terminated based on a determination of the CSA that further possession of classified matter by the facility would not be in the interest of the national security, the facility shall, upon notice from the CSA, immediately deliver all classified documents and materials to the Commission along with a certification of non-possession of classified information.

[62 FR 17697, Apr. 11, 1997]

**§95.55 Continued applicability of the regulations in this part.**

The suspension, revocation or other termination of access authorization or the termination of facility clearance does not relieve any person from compliance with the regulations in this part.

[62 FR 17698, Apr. 11, 1997]

**§95.57 Reports.**

Each licensee or other person having a facility clearance shall immediately report to the CSA and the Regional Administrator of the appropriate NRC Regional Office listed in appendix A, 10 CFR part 73:

(a) Any alleged or suspected violation of the Atomic Energy Act, Espionage Act, or other Federal statutes related to classified information.

(b) Any infractions, losses, compromises or possible compromises of classified information or classified documents not falling within paragraph (a) of this section.

(c) In addition, an authorized classifier of a licensee, certificate holder or other organization subject to this part shall complete an NRC Form 790, "Classification Record," whenever matter containing classified information is generated, its classification changed or it is declassified. Notification of declassification is not required for any document or material which has an automatic declassification date. Completed NRC Form 790 must be submitted to the NRC Division of Security, Washington, DC 20555-0001, on a monthly basis.

[62 FR 17698, Apr. 11, 1997]

**§95.59 Inspections.**

The Commission shall make inspections and reviews of the premises, activities, records and procedures of any person subject to the regulations in this part as the Commission and CSA deem necessary to effect the purposes of the Act, E.O. 12958 and/or NRC rules.

[62 FR 17698, Apr. 11, 1997]

VIOLATIONS

**§95.61 Violations.**

(a) The Commission may obtain an injunction or other court order to prevent a violation of the provisions of—

(1) The Atomic Energy Act of 1954, as amended;

(2) Title II of the Energy Reorganization Act of 1974, as amended; or

(3) A regulation or order issued pursuant to those Acts.

(b) The Commission may obtain a court order for the payment of a civil penalty imposed under section 234 of the Atomic Energy Act:

(1) For violations of—

(i) Sections 53, 57, 62, 63, 81, 82, 101, 103, 104, 107, or 109 of the Atomic Energy Act of 1954, as amended;

(ii) Section 206 of the Energy Reorganization Act;

(iii) Any rule, regulation, or order issued pursuant to the sections specified in paragraph (b)(1)(i) of this section;



## Nuclear Regulatory Commission

## § 100.2

(iv) Any term, condition, or limitation of any license issued under the sections specified in paragraph (b)(1)(i) of this section.

(2) For any violation for which a license may be revoked under Section 186 of the Atomic Energy Act of 1954, as amended.

[57 FR 55080, Nov. 24, 1992]

### § 95.63 Criminal penalties.

(a) Section 223 of the Atomic Energy Act of 1954, as amended, provides for criminal sanctions for willful violation of, attempted violation of, or conspiracy to violate, any regulation issued under sections 161b, 161i, or 161o of the Act. For purposes of section 223, all the regulations in part 95 are issued under one or more of sections 161b, 161i, or 161o, except for the sections listed in paragraph (b) of this section.

(b) The regulations in part 95 that are not issued under sections 161b, 161i, or 161o for the purposes of section 223 are as follows: §§95.1, 95.3, 95.5, 95.7, 95.8, 95.9, 95.11, 95.17, 95.19, 95.21, 95.23, 95.55, 95.59, 95.61, and 95.63.

[57 FR 55080, Nov. 24, 1992]

## PART 100—REACTOR SITE CRITERIA

Sec.

100.1 Purpose.

100.2 Scope.

100.3 Definitions.

100.4 Communications.

100.8 Information collection requirements: OMB approval.

### Subpart A—Evaluation Factors for Stationary Power Reactor Site Applications Before January 10, 1997 and for Testing Reactors

100.10 Factors to be considered when evaluating sites.

100.11 Determination of exclusion area, low population zone, and population center distance.

### Subpart B—Evaluation Factors for Stationary Power Reactor Site Applications on or After January 10, 1997

100.20 Factors to be considered when evaluating sites.

100.21 Non-seismic site criteria.

100.23 Geologic and seismic siting criteria.

## APPENDIX A TO PART 100—SEISMIC AND GEOLOGIC SITING CRITERIA FOR NUCLEAR POWER PLANTS

AUTHORITY: Secs. 103, 104 161, 182, 68 Stat. 936, 937, 948, 953, as amended (42 U.S.C. 2133, 2134, 2201, 2232); sec. 201, as amended, 202, 88 Stat. 1242, as amended, 1244 (42 U.S.C. 5841, 5842).

SOURCE: 27 FR 3509, Apr. 12, 1962, unless otherwise noted.

### § 100.1 Purpose.

(a) The purpose of this part is to establish approval requirements for proposed sites for stationary power and testing reactors subject to part 50 or part 52 of this chapter.

(b) There exists a substantial base of knowledge regarding power reactor siting, design, construction and operation. This base reflects that the primary factors that determine public health and safety are the reactor design, construction and operation.

(c) Siting factors and criteria are important in assuring that radiological doses from normal operation and postulated accidents will be acceptably low, that natural phenomena and potential man-made hazards will be appropriately accounted for in the design of the plant, that site characteristics are such that adequate security measures to protect the plant can be developed, and that physical characteristics unique to the proposed site that could pose a significant impediment to the development of emergency plans are identified.

(d) This approach incorporates the appropriate standards and criteria for approval of stationary power and testing reactor sites. The Commission intends to carry out a traditional defense-in-depth approach with regard to reactor siting to ensure public safety. Siting away from densely populated centers has been and will continue to be an important factor in evaluating applications for site approval.

[61 FR 65175, Dec. 11, 1996]

### § 100.2 Scope.

The siting requirements contained in this part apply to applications for site approval for the purpose of constructing and operating stationary power and